



hp industry
standard servers

november 2002



technical
white paper

initial deployment of the ProLiant Support Pack using Insight Manager 7

table of contents

abstract	2
overview	2
pre-requisites for installation of ProLiant Support Packs	3
Microsoft Windows 2000	3
Microsoft Windows NT 4.0	3
obtaining the appropriate ProLiant Support Pack	4
Copying Components from the SmartStart CD	4
Copying components from the HP website	5
configuring the ProLiant Support Pack for distribution	7
Configuring the ProLiant Support Pack for SmartStart 5.50 or later	7
Configuring the Compaq Support Paq for SmartStart 5.40 or earlier	11
running Insight Manager 7 as a Windows user	14
Microsoft Windows 2000	14
configuring and executing the Application Launch Task	17
confirming execution of the Application Launch Task	20
Using the Smart Component Installation Log	20
appendix A – an alternative batch file	22
Running SWUpdate.bat	22
Alternative to swupdate.bat	22
Choosing the appropriate batch file	23

abstract

Insight Manager 7™ provides compelling new functionality for system software maintenance and important improvements in security. These features require installation of the ProLiant Support Pack for Microsoft Windows 2000 (version 5.14A or greater) or the ProLiant Support Pack for Microsoft Windows NT (version 1.10A or greater) on managed systems. This document describes the process for carrying out the initial deployment of ProLiant Support Packs to groups of ProLiant servers using the Insight Manager 7 application launch task.

overview

Insight Manager™ 7 provides compelling new functionality for system software maintenance and important improvements in security. Insight Manager 7, in concert with the Version Control Agent and the Version Control Repository Manager, allows systems administrators to manage versions of HP system software according to user-defined baselines. It also enables remote updates of BIOS, drivers, and management agents across groups of *ProLiant™* servers. These capabilities significantly reduce the time and expense associated with maintaining consistent, well-tested system software configurations across the enterprise.

Insight Manager 7, as well as the HP Insight Management Agents for Microsoft Windows 2000 and Microsoft Windows NT (version 5.3 or greater) and the Version Control Agent, provide support for industry standard Secure Sockets Layer (SSL) and secure task execution. SSL ensures that all management communications over HTTP are encrypted and private. Secure task execution ensures that only trusted Insight Manager 7 servers are able to perform state changing tasks such as system software deployments.

To take advantage of these new capabilities, it is necessary to install the HP Insight Management Agents for Microsoft Windows 2000 and Microsoft Windows NT (version 5.3 or greater) and the Version Control Agent on each managed Microsoft Windows system. This document describes the process for rolling out the ProLiant Support Packs (PSP) containing these components to groups of ProLiant servers using the application launch task in Insight Manager 7. The process is broken into six steps, outlined below:

1. Check the installation prerequisites for the ProLiant Support Pack.
2. Obtain the appropriate ProLiant Support Pack(s).
3. Configure the ProLiant Support Pack (s) for distribution.
4. Configure Insight Manager 7 to run in the context of a Microsoft Windows administrator.
5. Configure and execute the Insight Manager 7 application launch task if not already done.
6. Confirm execution of the application launch task.

After the successful completion of all of the above steps, the proper version of the HP Insight Management Agents and the Version Control Agent will be installed on each target system.

pre-requisites for installation of ProLiant Support Packs

In order to install the Management Agents, the SNMP service must be installed and running on each target server. In addition, the ability to use advanced functionality such as group configuration requires an SNMP community string configured with read/create privileges. The Management Agents will use this community string.

Follow the steps below to configure SNMP.

Microsoft Windows 2000

1. Select **Start** → **Settings** → **Control Panel** → **Add/Remove Programs**.
2. From **Add/Remove Programs**, click **Add Remove Windows Components**, and then select **Management and Monitoring Tools**. This selects all three sub-components. If you need to select SNMP individually, click **Details**, then select **SNMP**. Click **OK**, then select **Next** to install SNMP.
3. Once SNMP is installed, select **Start** → **Programs** → **Administrative Tools** → **Services** → Right click on **SNMP Service** → and select **Properties**.
4. Select the **Security** tab to edit the community string and rights for settings appropriate for your environment.

Microsoft Windows NT 4.0

1. Select **Start** → **Settings** → **Control Panel** → **Network**.
2. Select the **Services** tab. If the SNMP service is not installed, click **Add** to install it and then reboot your system.
3. Go back into **Start** → **Settings** → **Control Panel** → **Network** and select the Network tab. In the **Network Service** box, select **SNMP Service**, and then click **Properties**.
4. Edit the community string and rights for settings appropriate for your environment.

NOTE: After you initially install SNMP, you will need to reinstall any Microsoft Windows service packs.

obtaining the appropriate ProLiant Support Pack

HP provides three methods for obtaining the ProLiant Support Packs:

- SmartStart CD
- HP website
- ActiveUpdate

This section will discuss how to copy components from the SmartStart CD and download components from the HP website. For instructions on how to install and configure ActiveUpdate, refer to *ActiveUpdate User Guide* located on the Management CD.

NOTE: This section assumes that Insight Manager 7 is already installed on your server.

Copying Components from the SmartStart CD

The SmartStart CD is a convenient source of system software for systems administrators that may not have access to the Internet from within their company datacenter. The following steps outline the process for copying software from the SmartStart CD to a directory on the Insight Manager 7 server. The Insight Manager 7 application launch task will deploy the software contained in this directory.

1. Create a directory on the Insight Manager 7 server named `c:\pspinstall`.

NOTE: For this section, we will use the example `c:\pspinstall` as the directory for the components.

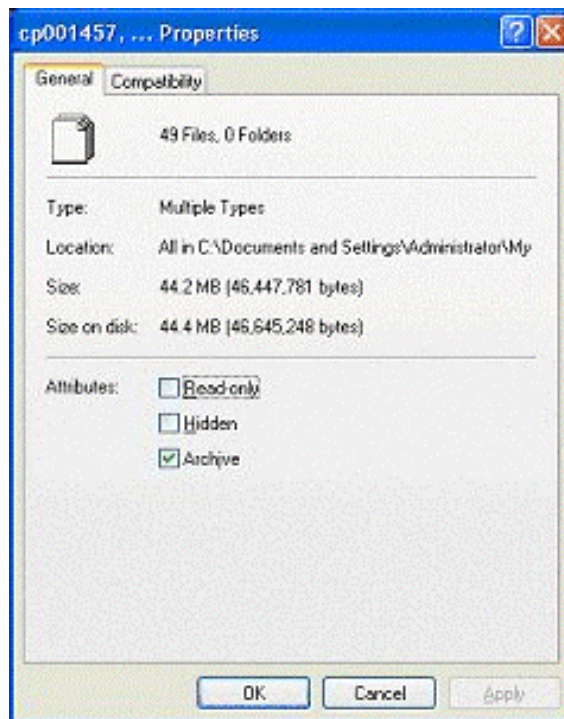
2. Insert the SmartStart CD into the CD-ROM drive. Read and accept the license agreement. Close the dialog box.
3. From Windows Explorer, expand the SmartStart CD to view all of the directories. If the License Agreement is displayed again, close the dialog box. If you are using SmartStart 5.5 or earlier, a popup message is displayed telling you that if you continue you will exit the SmartStart System Utility, click **OK**.
4. Copy the contents of the `\Compaq\csp\nt` directory to `c:\pspinstall`. If you are using SmartStart 5.5 or earlier, copy the contents of the `\CPQSUPSW\NTCSP` directory to `c:\pspinstall`. This step will ensure that all Microsoft Windows 2000, Microsoft Windows NT, and Microsoft Windows .NET beta components are copied to the `c:\pspinstall` directory.

NOTE: Copy only the contents of the `\compaq\csp\nt` directory (or the `\CPQSUPSW\NTCSP` directory) to `c:\pspinstall`, not the entire directory structure. In other words, the components in `\compaq\csp\nt` (or in `\CPQSUPSW\NTCSP`) should appear in `c:\pspinstall`, not in `c:\pspinstall\nt` (or in `c:\pspinstall\ntcsp`).

5. Remove write protection from all components in `c:\pspinstall`.
 - a. In Explorer, expand `c:\pspinstall`, and highlight any one of the files.
 - b. Press the **Ctrl+A** keys to select all the components.
 - c. Right-click on a single component, click **Properties**, and then deselect **Read**

Only, and click **Apply**.

d. Click **OK**.



Copying components from the HP website

The HP website provides convenient access to the latest HP system software. The site is conveniently laid out so that system administrators can choose software by server type and operating system.

NOTE: If you are getting your components from the SmartStart CD, then you can skip this section and go to Configuring the ProLiant Support Pack for Distribution.

1. Create a directory on the Insight Manager 7 server named `c:\pspinstall`.
2. Browse to www.compaq.com/support and select **software & drivers**. From the **servers** column, click **ProLiant**.
3. In Option 2, from the **operating system** drop-down menu, select either **Microsoft Windows 2000** or **Microsoft Windows NT 4.0**. From the **Category** drop-down menu, select Support Pack.

option 1:

locate by product

select the product, model/processor, and operating system

product

ProLiant BL20p

model or processor

All Models

operating system

Microsoft Windows 2000

locate software >>

option 2:

locate by category

select the operating system and software category

operating system

Microsoft Windows 2000

category

All Categories

locate software >>

4. Click **locate software**.
5. The **software and drivers** page is displayed. Select the appropriate Support Pack on the support pack page that is displayed.
6. A security warning dialog box is displayed. Click **Yes**.
7. Click **download**, and when prompted, select the target directory as c:\pspininstall. Click **Save**. The bundle will then transfer to the c:\pspininstall directory.

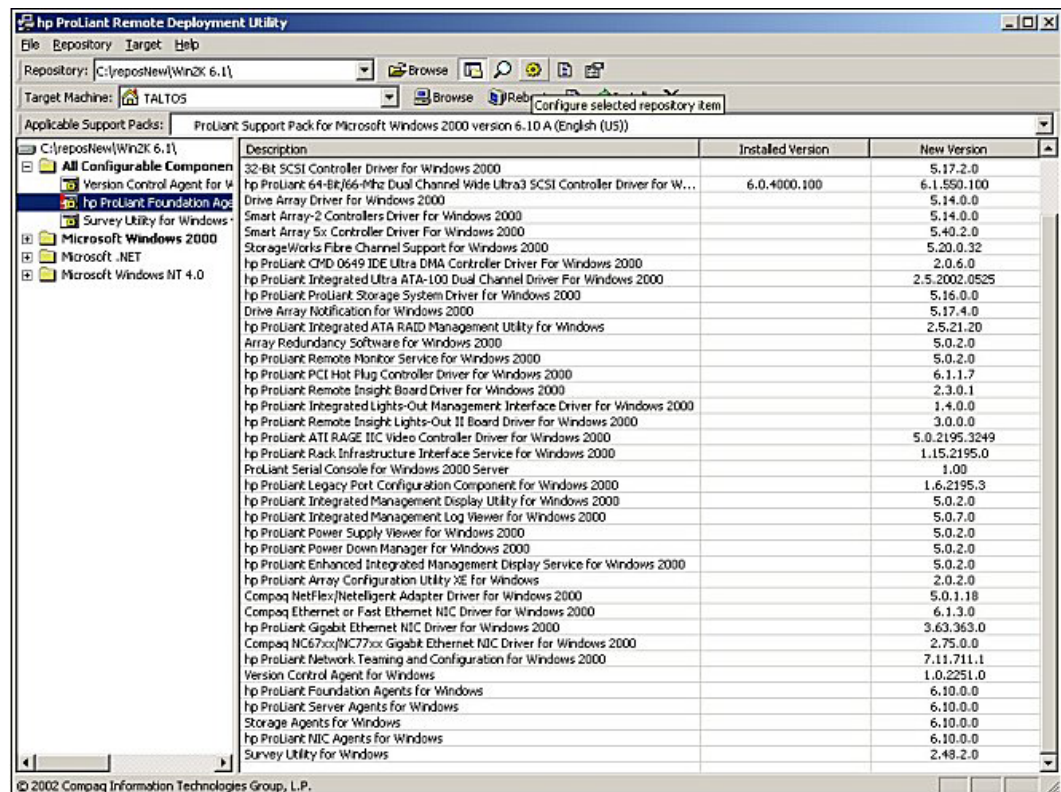
configuring the ProLiant Support Pack for distribution

Configuring the ProLiant Support Pack ensures that the Management Agents and Version Control Agent are installed with the correct password and will trust the proper Insight Manager 7 management server. ProLiant Support Pack configuration is done in one of two ways, depending on the version of SmartStart you use. If you have SmartStart 5.50 or later, you will configure your ProLiant Support Pack with the Remote Deployment Utility distributed with the ProLiant Support Packs for Microsoft Windows 2000 and Microsoft Windows NT (version 5.50 or greater, for both). If you are using SmartStart 5.40 or earlier to configure the ProLiant Support Pack, you will use the Component Configuration Tool that was distributed with the ProLiant Support Packs for Microsoft Windows 2000 (version 5.14 to 5.40) and Microsoft Windows NT (version 1.10 to 5.40).

Configuring the ProLiant Support Pack for SmartStart 5.50 or later

From the c:\pspinstall directory, launch SETUP.EXE to configure the components that will be distributed to the target system. The **ProLiant Remote Deployment Utility** is displayed.

1. Expand the **All Configurable Components** section and right-click on **Foundation Agents for Windows**, then click **Configure...**



2. The **Item Configuration** page is displayed. Scroll down to the **SNMP Settings** section. You will need to select **Enable SNMP Sets** in order to use group configuration, clear the Integrated Management Log, or change management agents' settings. You may also want to select **Enable Remote Reboot** or change the time in the **Data Collection Interval** drop-down list.

SNMP Settings

The Agents have several SNMP settings that control data collection:

Data Collection Interval:

☒ Enable SNMP Sets

☒ Enable Remote Reboot (only available if SNMP Sets are enabled)

3. Scroll down to the **Web-Based System Security Setup** section. You will need to configure the administrator password governing access to the agents such as the Management Agent and the Version Control Agent. This is a required operation whether overwrite is selected or not. Select **Overwrite existing Web-Based System Security Settings** if you plan to deploy the new ProLiant Support Pack to a system with an older version of Management Agents but want to enforce the new password setting. Configuration of trust relationships also requires the overwrite option to be selected.

The security settings below must be configured for all HP web-based software. The administrator password must be set for web-based software to function. The trust relationship must be configured order for the device to interoperate with Insight Manager. Please configure these settings below:

Note: If the device already has a password set on the server, the overwrite setting must be checked any new password/trust relationship settings to be configured successfully.

☒ **Overwrite existing HP Web-Based System Security Settings**

Administrator Password	
<i>Note: This password will also be set for the 'Operator' and 'User' accounts if they do not already have passwords.</i>	
Password:	<input type="text"/> (required)
Confirm:	<input type="text"/> (required)
Operator Password	
Password:	<input type="text"/>
Confirm:	<input type="text"/>
<i>The Administrator password will be used here.</i>	
User Password	
Password:	<input type="text"/>
Confirm:	<input type="text"/>
<i>The Administrator password will be used here.</i>	

4. Scroll down to the **Insight Manager 7 Trust Relationship** section. From the **Select Trust Mode** box, select **Trust by Certificate**.

5. Paste the Insight Manager 7 certificate into the designated space. To acquire the Insight Manager 7 certificate:
 - a. Open a new browser page and log into your Insight Manager 7 server.
 - b. Select **Settings** → **Security** → **Certificate Lists**. Enter the keystore password you entered during installation of Insight Manager 7. If you are using Insight Manager 7 SP1 or greater, a keystore password is not required. Refer to the *Insight Manager 7 User Guide* located on the Management CD (version 5.40 or greater).
 - c. From the **Actions** column in the **Server Certificate** table, select the icon to export the server certificate. When prompted, save the file to your desktop.

From this page you can export (📄) the Server Certificate, import certificates into the Trusted Certificates List, delete (X) certificates from the Trusted Certificates List, and export (📄) certificates from the Trusted Certificates List.

Server Certificate				
Actions	Alias	Issued By	Issued To	Expiration
📄	servercertificate			February 21, 2012

Trusted Certificates					Import
Actions	Alias	Issued By	Issued To	Expiration	

- d. From your desktop, right-click on the server certificate file, select **Open With**, and then click **Notepad**.
- e. Highlight all the text and press the **Ctrl+C** keys to copy it to the clipboard.
- f. Return to the **Configuration Item** page in the **Proliant Remote Deployment Utility**. Paste the certificate into the **Insight Manager 7 Trust Relationship** text box by pressing the **Ctrl+V** keys to paste the certificate.

Insight Manager 7 Trust Relationship

Note: For establishing the trust relationship with a new Insight Manager 7 server, you must check the 'Overwrite security setting checkbox' above.

Select Trust Model: **Trust By Certificate**

The server will only accept Secure Task Execution requests and Single Login requests that have been signed by a Insight Manager 7 server with a Trusted Certificate. Cut and paste the base64 encoded certificate into the text box below:

```
-----BEGIN CERTIFICATE-----
MIICWjCCAcMCBD1O1W4wdQYKJoZ1hvcNAQEFBQAwdEQMA4GA1UEBxMHSG91c3Rvb3gEOmAwGA1UE
CBMFVGV4YXhXc2A3BgnVBAYTA1VTMQ8wDQYDVQQKEwZDb21wYXExITafBgNVBAsTGENTPVBVBUSBj
bnNpZ2h0IE1hbmFnZXIqNzEPMA0GA1UEAxMGEVFMVE9TMB4XDTYtYMDgwNTE1MTAzOFoXDTEyYMDgw
NTE1MTAzOFowDQEMA4GA1UEBxMHSG91c3Rvb3gEOmAwGA1UECBMFVGV4YXhXc2A3BgnVBAYTA1VT
MQ8wDQYDVQQKEwZDb21wYXExITafBgNVBAsTGENTPVBVBUSBjbnNpZ2h0IE1hbmFnZXIqNzEPMA0GA1
UEAxMGEVFMVE9TMB4XDTYtYMDgwNTE1MTAzOFoXDTEyYMDgwNTE1MTAzOFowDQEMA4GCSqGSIBo3DQEB
AQUAA4GNADCBjQKBgcQVjCZft5eFR8R2FRoadVUUG
UePGrQc6yXez1mjVjVp8b0UECmpsaDt7WtN5hX4NYpdusn4J1K0ZF1EM29Gft1kjhvr9KMGuG
D2M7HMS31tLpUrhPvHeZ8BHhNqX1Ivqz1wr/tEnTvY8uX/NGFv1eRLxYrvjR66gRsfIn2gnx5w1d
AQA8MA0GCSqGSIBo3DQEBBQAUA4GBABjSBSHdgRnhYXK8jha08xc2HfWfnHfU0hkACPFx1O4VPKW2
WwNvjIgs8Br5726f0P4/CA/YhN1gvjJDEwg8hootd3uqy5xy/IK3Cy/3oRb7FR9BjZucUgV/bkQc
NICj4eeXKczSYu7tJmKur+x2GMhQujOokOiv1BLV7Bw6f1B
-----END CERTIFICATE-----
```

- Click **Save** to finish configuring the component. The **Remote Deployment Utility** page is displayed showing that the red exclamation point next to the Foundation Agent icon is gone and has been replaced with a blue check mark signifying that it has been configured.
- Next, you may optionally choose to configure the Version Control Agent. If you choose

to omit this step, you will be able to use Insight Manager 7 group configuration to configure the Version Control Agent on all of your systems once the ProLiant Support Pack installation has completed.

- a. From the **ProLiant Remote Deployment Utility** (SETUP.EXE) expand the **All Configurable Components** section and right-click **Version Control Agent for Windows** and select **Configure**.
- b. The **Item Configuration** page is displayed. Scroll down to the **Version Control Agent Setup** section. Enter the server name on which the Version Control Repository Manager is installed and enter the administrator password used to log on to the Version Control Repository Manager.

Compaq Version Control Agent Setup

Compaq Version Control Repository Manager

Server Name:

Administrator Password:

- c. Scroll down to the **Web-Based Management Setup** section and enter the same password and **Insight Manager 7 certificate** used when configuring the Foundation Agents. This step is required because the Foundation Agents and the Version Control Agent each have their own Web server and may be installed independently of each other.
- d. Click **Save** to create the updated component. A pop-up message is displayed, telling you that it is writing the configuration.

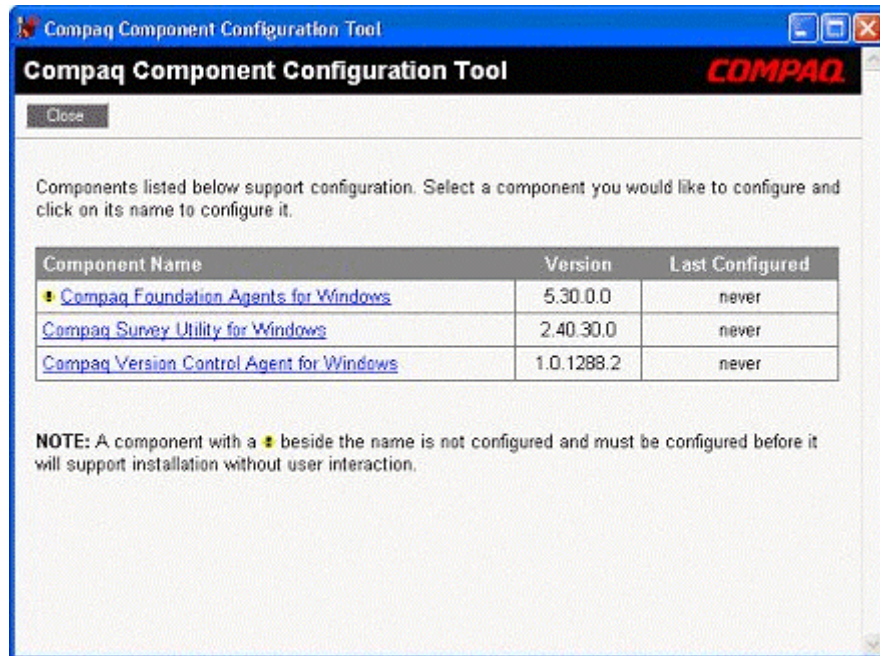
You are now ready to proceed to Running Insight Manager 7 as a Windows User.

NOTE: If you plan to deploy multiple Version Control Repository Managers, it may be preferable to configure the reference Version Control Repository Manager following the deployment of the ProLiant Support Pack. Simply use Insight Manager 7 group configuration to configure the set of systems that will point to each Version Control Repository Manager. Instructions for using group configuration are documented in the *Insight Manager 7 Technical Reference Guide* located on the Management CD (version 5.30 or greater).

Configuring the Compaq Support Paq for SmartStart 5.40 or earlier

Launch CPCONFIG.EXE to configure the components that will be distributed to the target system. CPCONFIG.EXE is copied to the c:\pspinstall install directory along with the other components in the Compaq Support Paq. The **Compaq Component Configuration Tool** page is displayed.

1. From the **Component Name** table, click **Compaq Foundation Agents for Windows**.



2. The **Compaq Foundation Agents for Windows Configuration** page is displayed. Scroll down to the **SNMP Settings** section. You will need to **Enable SNMP Sets** in order to use group configuration, clear the Integrated Management Log, or change management agents' settings. You may also want to select **Enable Remote Reboot** or change the time in the **Data Collection Interval** drop-down list.

SNMP Settings

The Agents have several SNMP settings that control data collection:

Data Collection Interval: 2 minutes ▼

☒ Enable SNMP Sets

☒ Enable Remote Reboot (only available if SNMP Sets are enabled)

3. Scroll down to the **Compaq Web-Based Management Setup** section. You will need to configure the administrator password governing access to the agents such as the Compaq Management Agents and the Compaq Version Control Agent. This is a required operation whether overwrite is selected or not. Select **Overwrite existing Compaq Web-Based Management security settings** if you plan to deploy the new CSP to a system with an older version of Compaq Management Agents but want to enforce the new password setting. Configuration of trust relationships also requires

the overwrite option be selected.

Compaq Web-Based Management Setup

Security settings must be configured for any server installed with Compaq web-based applications. Please configure these settings below.

Note: Check the following box to overwrite existing Web-Based Management security settings for a previously configured server.

☒ **Overwrite existing Compaq Web-Based Management security settings.**

Administrator Password

Note: This password will also be set for the 'Operator' and 'User' accounts if they do not already have passwords.

Password:

Confirm:

4. Scroll down to the **Compaq Insight Manager 7 Trust Relationship** section. From the Select Trust Mode drop-down menu, select **Trust by Certificate**.
5. Paste the Compaq Insight Manager 7 certificate into the designated space. To acquire the Compaq Insight Manager 7 certificate:
 - a. Open a new browser window and log into your Compaq Insight Manager 7 server.
 - b. Select **Settings → Security → Certificate Lists**. Enter the keystore password you entered during installation of Compaq Insight Manager 7. If you are using Compaq Insight Manager 7 SP1 or later a keystore password is not required. Refer to the *Compaq Insight Manager User Guide* located on the Compaq Management CD (version 5.40 or greater).
 - c. From the **Actions** column in the **Server Certificate** table, select the icon to export the server certificate. When prompted, save the file to your desktop.

From this page you can export (📄) the Server Certificate, import certificates into the Trusted Certificates List, delete (X) from the Trusted Certificates List, and export (📄) certificates from the Trusted Certificates List.

Server Certificate				
Actions	Alias	Issued By	Issued To	Expiration
📄	servercertificate			February 21, 2012

Trusted Certificates				
Actions	Alias	Issued By	Issued To	Expiration

- d. From your desktop, right-click on the server certificate file, select **Open With**, and then click **Notepad**.
- e. Highlight all of the text and press the **Ctrl+C** keys to copy it to the clipboard.
- f. Return to the **Compaq Component Configuration Tool** and paste the certificate into the **Compaq Insight Manager 7 Trust Relationship** text box by pressing the **Ctrl+V** keys to paste the certificate.

Compaq Insight Manager 7 Trust Relationship

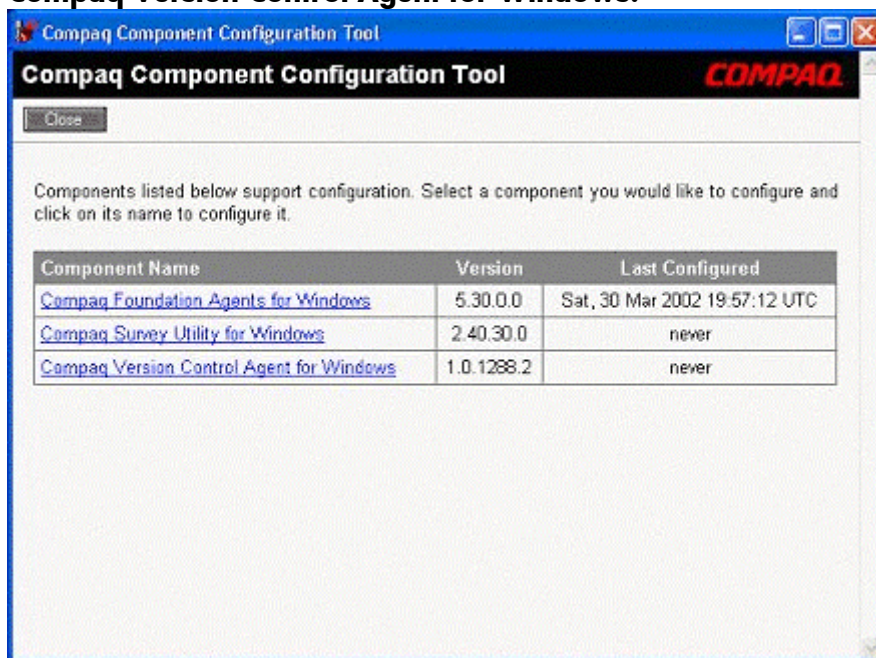
Note: For establishing the trust relationship with a new Compaq Insight Manager 7 server, you must check the 'Overwrite security setting above.

Select Trust Mode: Trust By Certificate ▼

The server will only accept Secure Task Execution requests and Single Login requests that have been signed by a Compaq Insight Manager Trusted Certificate. Cut and paste the base64 encoded certificate into the text box below.

-----BEGIN CERTIFICATE-----
MIICXDCCACUCBxDd8KwDQYKoZIHvcNAQEVBQAwDETCAAGAIUEBAHNSG91c3RvbzEOMAwGA1UE
CBNFVGU4YXNkCzAxBgNVBAYTA1VTRGSwDQYDVQQKEwZDb21wYXNlITAtBgNVBAsTGENTPVBBSUBJ
bnNpZ2hoIE1ubmFuzXIqNzEQMA4GA1UEAxMHQCOINWLNQNTAEFwOeEjAyMjEwNDExOTdaFe0xMjAy
MjEwNDExOTdaMHUwEDABgNVBAcTB0hvdiZNOUy24xODpANBgNVBAgTBVRleGFzMQswCQYDVQQGEwJV
UzEPMAAGA1UEChNGQ292tGfXNSERwYDVQLExhDT01QQVEgSW5zaWdodCBENVYSh22VyIDexEDA
BgNVBAMTBOMJTTTUDEIwZS8wDQYKoZIHvcNAQEVBQADgYOAAGIJJLoGBAHNYnQgwvZj7vgjdQJ2
YRCx91IU1u6gnXBf20w9sX7PfB8b1q2PjAYHemSENPu7f45tcIKtk1Vp3pLAKCNL29zVRK/Oal1P
KciRrK071ULULcmqMCIG6RUT4t6FcpwP/yhOf7XR9LCARR9qcb7NPgOBpTQBlo1FEAG2GSKZ
AgNBAAEWdQYKoZIHvcNAQEVBQADgYEAAJOsk4hYL5TepWtmSSIQSG5NFZ/fOEbgne+Q7j6b3Es
uYVPr42xmHmw+QRvgqtTgmPyYhaRp1a4VsorUGVEhHfi2ko82pX1N55dmly1vFBIVBEit5jXlm
B5br1WmNHNvN/QVSLfaABvAjGwClMnS5U9BIN1hrKck+WqEK8Ug=
-----END CERTIFICATE-----

6. Click **Save** to finish configuring the component. A pop-up message is displayed, telling you that the configuration was updated successfully. Click **OK**.
7. Next, you may optionally choose to configure the Compaq Version Control Agent. If you choose to omit this step, you will be able to use Compaq Insight Manager 7 group configuration to configure the Compaq Version Control Agent on all your managed devices once the CSP installation has completed.
 - a. From the **Compaq Component Configuration Tool** (CPCONFIG.EXE) click **Compaq Version Control Agent for Windows**.



- b. The **Compaq Version Control Agent for Windows Configuration** page is displayed. Scroll down to the **Compaq Version Control Agent Setup** section, enter the server name on which the Compaq Version Control Repository Manager is installed and enter the administrator password used to log on to the Compaq Version Control Repository Manager.

Compaq Version Control Agent Setup

Compaq Version Control Repository Manager

Server Name:
Administrator Password:

- c. Scroll down to the **Compaq Web-Based Management Setup** section and enter the same password and Compaq Insight Manager 7 certificate used when configuring the Compaq Foundation Agents. This step is required because the Compaq Foundation Agents and the Compaq Version Control Agent each have their own Web server and may be installed independently of each other.
- d. Click **Save** to create the updated component. A pop-up message is displayed, telling you that the configuration was updated successfully. Click **OK**.

You are now ready to proceed to Running Insight Manager 7 as a Windows User.

NOTE: If you plan to deploy multiple Compaq Version Control Repository Managers, it may be preferable to configure the reference Compaq Version Control Repository Manager following the deployment of the CSP. Simply use Compaq Insight Manager 7 group configuration to configure the set of systems that will point to each Compaq Version Control Repository Manager. Instructions for using group configuration are documented in the *Compaq Insight Manager 7 Technical Reference Guide* located on the Compaq Management CD (version 5.30 or greater).

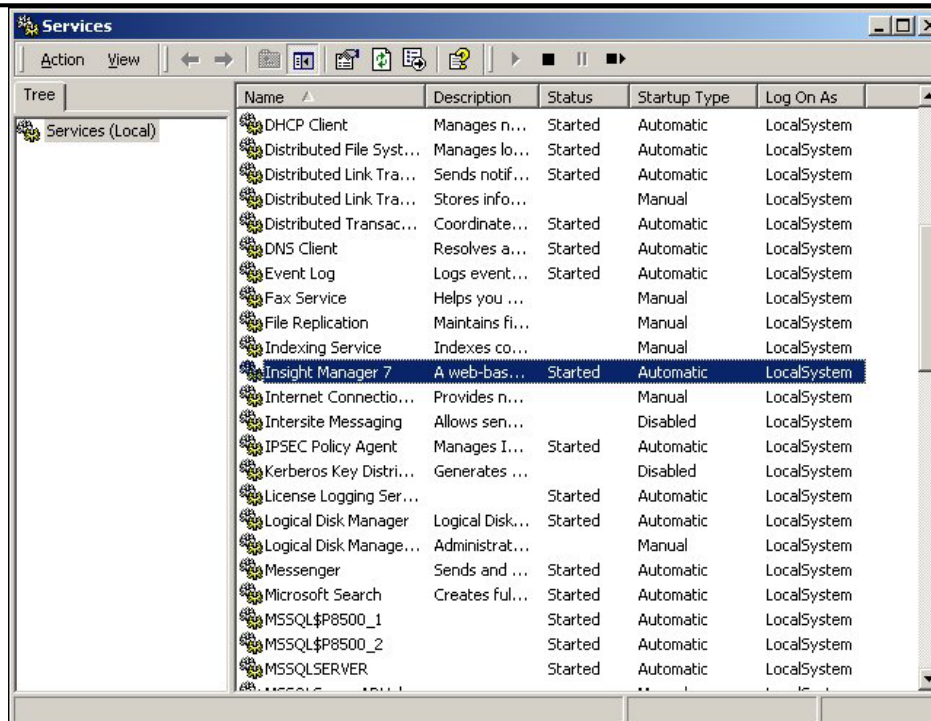
running Insight Manager 7 as a Windows user

In order to distribute ProLiant Support Packs using the Insight Manager 7 application launch task, it is necessary to configure the Insight Manager 7 service to run under the context of a user with administrative privileges for proper execution of setupc.exe (command line version of the ProLiant Remote Deployment Utility).

NOTE: If you are currently using Windows Authentication and you change the Insight Manager 7 service account, this account must have sufficient privileges to access the database.

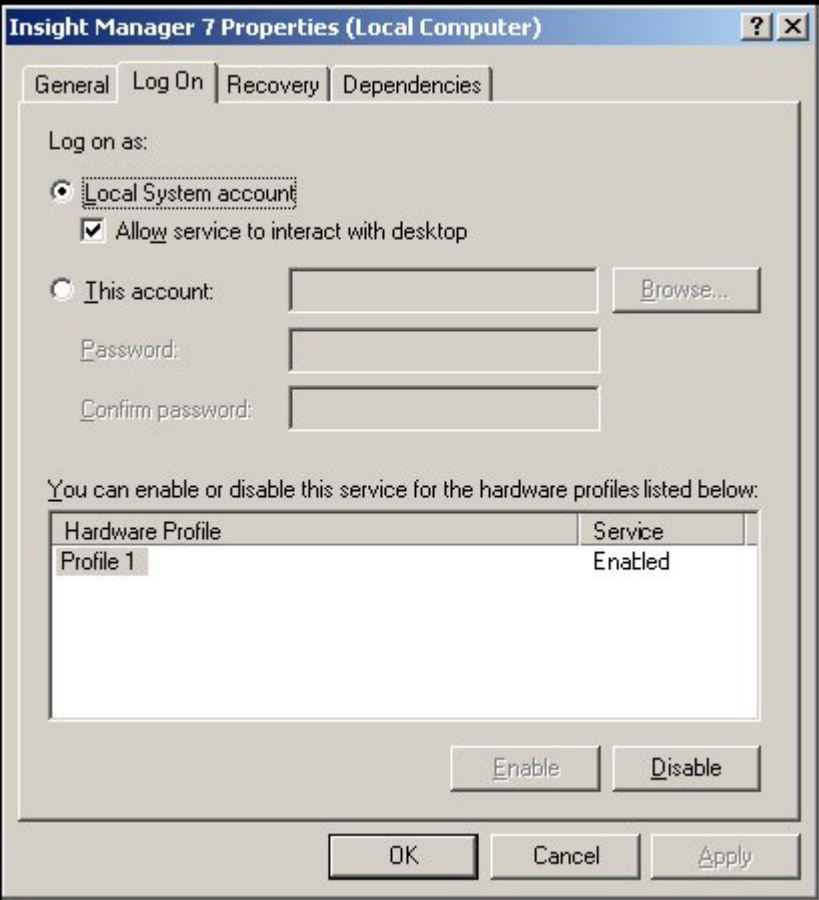
Microsoft Windows 2000

1. From **Start** → **Settings** → **Control Panel** → **Administrative Tools**, select **Services**, and then select **Insight Manager 7**.







2. Stop the **Insight Manager 7** service.
3. Right-click **Insight Manager 7** and select **Properties**.
4. From the **Properties** dialog box, select the **Log On** tab and then select **This account**. Browse and select a user, then enter the appropriate password, and then confirm the password. Click **OK**.

NOTE: It is necessary to configure the Insight Manager 7 service to run in the context of a user because the Local System account does not have sufficient privileges to authenticate to a remote device.



5. Restart the **Insight Manager 7** service. It should now be running in the context of the selected account. Close all windows.

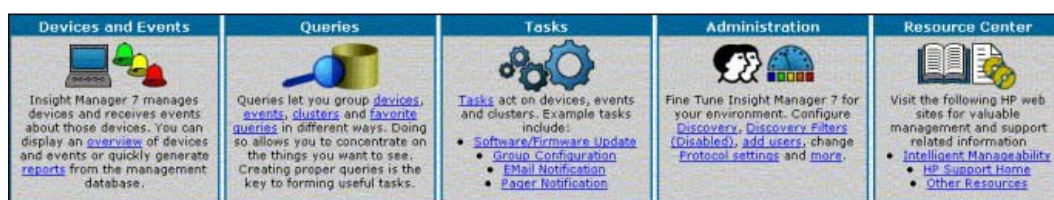
	Indexing Service	Indexes co...	Manual	LocalSystem
	Insight Manager 7	A web-bas...	Started Automatic	LocalSystem
	Internet Connectio...	Provides n...	Manual	LocalSystem
	Intersite Messaging	Allows sen...	Disabled	LocalSystem

configuring and executing the Application Launch Task

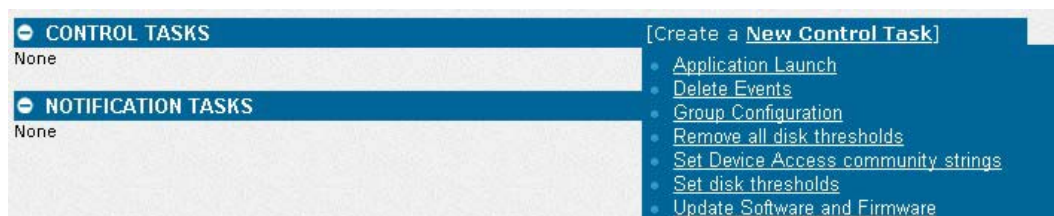
Now that the ProLiant Support Pack has been configured and Insight Manager 7 is running in the context of an administrator-level user, we are ready to configure the Insight Manager 7 application launch task that will deliver the ProLiant Support Pack to a set of systems identified in a query.

As part of the application launch task, users will enter the name of a batch file (swupdate.bat) and a set of variables that will be passed to the batch file. In order to authenticate to remote systems and deliver the ProLiant Support Pack payload, swupdate.bat calls setupc.exe (the command line version of the Remote Deployment Utility). As part of the application launch task, users will also define a set of target servers by selecting a query and determining the schedule on which the task will run.

1. Open a new browser and login to Insight Manager 7.
2. From the **Insight Manager 7** home page, select **Tasks** in the **Tasks** portion of the **QuickLinks** section.



3. Next, select **New Control Task**; then select **Application Launch** link.



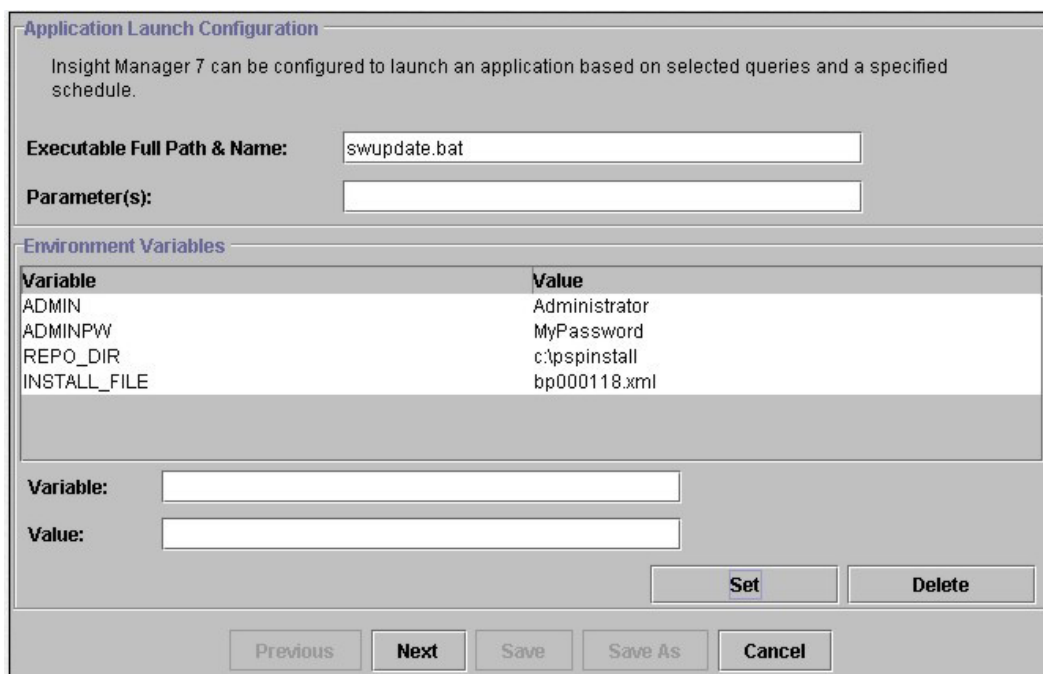
4. To configure the application launch task, follow the procedure listed below.
 - a. Enter SWUPDATE.BAT as the executable name (it is not necessary to include the full path).
 - b. Leave the **Parameter(s)** field blank.
 - c. Enter the variables with their associated values from the **Variable and Values** table by using the **Variable** and **Value** fields, then click **Set**.

Variable	Value
ADMIN	Username to use to connect to the remote system, this account has to have administrator privileges on the target system
ADMINPW	Password of the above account
REPO_DIR	Directory with the Support Pack (c:\pspinstall)
INSTALL_FILE	Name of bundle file to deploy – use the file bpXXXXXX.xml – look in the c:\pspinstall directory to find the filename to

use. The bundle file for version 5.14A of the Microsoft Windows 2000 Support Pack is bp000061.xml. For this white paper we are using bp000061.xml.

NOTE: Be sure to include the entire file name including the .xml suffix.

d. Click **Next**.



Application Launch Configuration

Insight Manager 7 can be configured to launch an application based on selected queries and a specified schedule.

Executable Full Path & Name:

Parameter(s):

Environment Variables

Variable	Value
ADMIN	Administrator
ADMINPW	MyPassword
REPO_DIR	c:\pspininstall
INSTALL_FILE	bp000118.xml

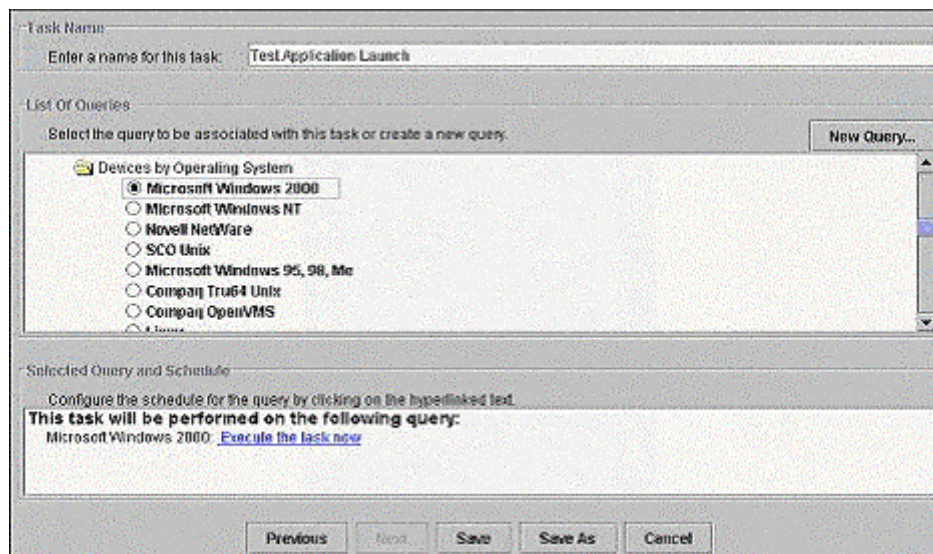
Variable:

Value:

Set **Delete**

Previous **Next** **Save** **Save As** **Cancel**

- From the **Create/Edit Task** page, enter a unique name for your application launch task, and then select a query that includes the set of devices you want to update with the new ProLiant Support Pack. If there are no existing queries that include the desired set of target systems, it is possible to create a new query by clicking **New Query**. The query creation wizard will lead you through the process of creating a query that suits your needs. For additional information on creating queries, refer to the *Insight Manager 7 Technical Reference Guide* located on the Management CD (version 5.30 or greater). Select **Schedule** in the **Selected Query and Schedule** section of the page.



Task Name

Enter a name for this task:

List Of Queries

Select the query to be associated with this task or create a new query. **New Query...**

Devices by Operating System

- ☒ Microsoft Windows 2000
- ☐ Microsoft Windows NT
- ☐ Novell NetWare
- ☐ SCO Unix
- ☐ Microsoft Windows 95, 98, Me
- ☐ Compaq Tru64 Unix
- ☐ Compaq OpenVMS
- ☐ Linux

Selected Query and Schedule

Configure the schedule for the query by clicking on the hypelinked text.

This task will be performed on the following query:

Microsoft Windows 2000: [Execute the task now](#)

Previous **Next** **Save** **Save As** **Cancel**

6. **The Schedule Configuration** page is displayed. Schedule the task to run at the appropriate time. To save the schedule selection, click **OK**.

Schedule Configuration

Query Driven Tasks:

- ☐ When new devices or events meet the query criteria
- ☐ When devices or events no longer meet the query criteria

Scheduled Tasks:

- ☒ Now
- ☐ Run periodically
- ☐ Run once

☐ Also run when system is started

Frequency

- ☐ Minute(s)
- ☐ Hourly
- ☐ Daily
- ☒ Weekly
- ☐ Monthly

Weekly

Every 1 week(s).

☐ Sun ☒ Mon ☐ Tue ☐ Wed ☐ Thur ☐ Fri ☐ Sat

Occurs at (HH:MM): 07:45 PM

☐ During the following times: [green denotes selected times]

Time Filters

Always

New... Edit...

Delete

am 12 1 2 3 4 5 6 7 8 9 10 11 12 pm 1 2 3 4 5 6 7 8 9 10 11 12 am

Mon Tue Wed Thu Fri Sat Sun

OK Cancel

Java Applet Window

7. Click **Save** to write the task to the Insight Manager 7 database.

NOTE: If you schedule your task to run **Now**, the task will execute shortly after it has been saved to the Insight Manager 7 database.

confirming
execution of the
Application
Launch Task

You have now completed the configuration and execution of the Insight Manager 7 application launch task. With logs provided by Insight Manager 7 and setupc.exe, you will now confirm whether the ProLiant Support Packs have installed on each of the target systems.

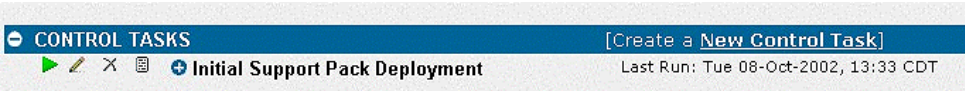
NOTE: Deploying a ProLiant Support Pack can take up to a half hour or longer, depending on the number of target devices. Even after Insight Manager 7 shows that the task is completed, the ProLiant Support Pack may still be installing on some target systems.

Using the Application Launch Log

Insight Manager 7 provides logs for all notification and control tasks including the application launch task. The application launch task log indicates whether the task has run against each of the target systems. It does not indicate whether the task has completed successfully. To understand whether the task has completed, refer to **Using the Smart Component Installation Log** section of this chapter.

To read the application launch task log:

- 1. From the **Insight Manager 7** home page, click **Tasks** in the **Tasks** portion of the **QuickLinks** section.
- 2. Click on the log icon associated with the application launch task that you created in the previous section.



- 3. From the **Query Results** page, click **Application Launch** in the **Event Type** column.

Actions ▾ View ▾						
State	Severity	Event Type	Device Name	Event Time	Assigned To	Comments
Not Cleared	✓	Application Launch	perf310	01-Oct-2002, 19:48:...	Assign to...	Add comments...

- 4. From the **Event** page, examine the contents of the log to determine whether the task has executed.

Application Launch Task Details		
80 Succeeded, 0 Failed		
Device	Severity	Details
10A	✓ Normal	The application launch was successful.
10GR	✓ Normal	The application launch was successful.
10H	✓ Normal	The application launch was successful.
10M	✓ Normal	The application launch was successful.
12EW	✓ Normal	The application launch was successful.
12FR	✓ Normal	The application launch was successful.
12GW	✓ Normal	The application launch was successful.
12R	✓ Normal	The application launch was successful.

Insight Manager 7 maintains a log in the batch file. To view this log, browse to the **log** subdirectory under the Insight Manager 7 directory.

The Version Control Agent on the target device also maintains an install log. You may view the batch file by accessing `https://devicename:2381/vcagent/installlog`.

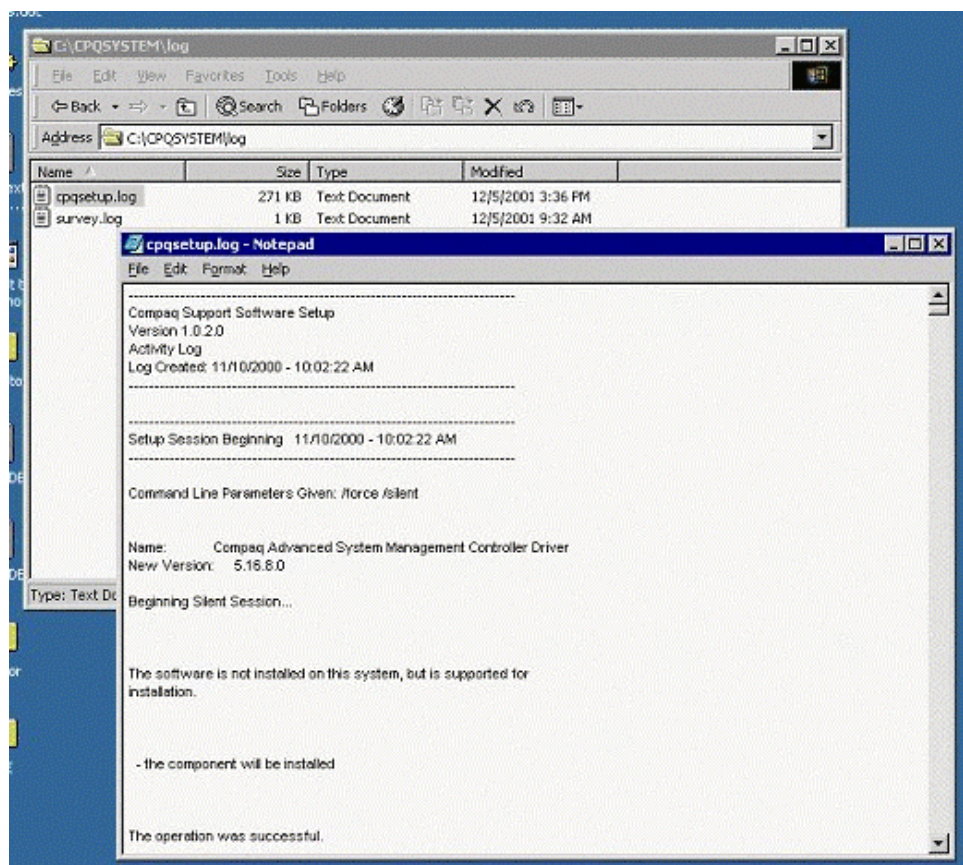
Using the Smart Component Installation Log

The Smart Component installation log provides detailed information concerning the success or

failure of each Smart Component installation that has been carried out on the system. To access the log, use Microsoft Terminal Services or map to the system drive on each of the systems whose log you wish to view. The log is located at %SystemDrive%\cpqsystem\log\cpqsetup.log. The log displays the installation results for each component.

NOTE: In many instances, several components from a ProLiant Support Pack will fail to install for the following reasons.

Typical reasons for failed component installations will be: up-to-date software is already installed on the target system, hardware or software dependencies are not met, or software is not needed for that particular server.



Conclusion

You have now successfully installed the ProLiant Support Pack on each of the systems selected in the Insight Manager 7 application launch task. Each system contains agents that support Secure Sockets Layer (SSL) and the Version Control Agent that will allow version control and remote update of BIOS, drivers and management agents. The trust relationship between each system and Insight Manager 7 has also been properly configured making it possible to carry out system software updates and group configuration tasks immediately.

For more information on the capabilities of Insight Manager 7 and other HP management tools, visit the HP website at www.hp.com/servers/manage.

appendix A – an alternative batch file

Running SWUpdate.bat

Swupdate.bat is the default batch file that installs with Insight Manager 7. It has advantages in that it allows users to deploy any Support Pack to any system provided the inclusion of the appropriate user name, password, ProLiant Support Pack name, and ProLiant Support Pack directory as task variables. The potential issue with this approach is that it requires users to input this information accurately, increasing opportunities for error. It also requires the user and password information to be stored in the Insight Manager 7 database.

The contents of the swupdate.bat file are printed here for your reference.

```
REM ***** HP SOFTWARE UPDATES *****

md log

echo ===== Begin ===== Device Name %deviceName% >> log\%deviceName%-
SWUpdate.log

echo Updating system software >> log\%deviceName%-SWUpdate.log

net use \\%devicename%\ipc$ /user:%admin% %adminpw%

%repo_dir%\setupc /f /t:%devicename% /r %repo_dir%\%install_file% >>
log\%deviceName%-SWUpdate.log

echo Installation complete >> log\%
%-SWUpdate.log

echo See the C:\CPQSYSTEM\LOG\CPQSETUP.LOG installation log file on server
%deviceName% for details. >> log\%deviceName%-SWUpdate.log

echo End ===== >> log\%deviceName%-SWUpdate.log

EXIT
```

Alternative to swupdate.bat

The following batch file may be used as an alternative to swupdate.bat. It assumes that the user account under which the Insight Manager 7 service is running will have sufficient administrative privileges on the remote system. It also assumes that a specific Support Pack (for example, Windows 2000 or Windows NT) will be deployed to each of the target systems and that the Support Pack exists in a predetermined directory.

While this batch file is less flexible than swupdate.bat, it does not require the user to configure any of the variables required by swupdate.bat. If the user copies this batch file to the directory containing swupdate.bat (c:\Program Files\HP\HP Insight Manager 7), it also becomes unnecessary to specify a path in addition to the name of the batch file (refer to the Application Launch Configuration screen capture earlier in this chapter).

The contents of the alternative batch file are listed below.

```
REM ***** HP SOFTWARE UPDATES ***** REM ***** f o r
```

```
echo ===== Begin ===== Device Name %deviceName% >> d:\data\%deviceName%-SWUpdate.log

echo Updating system software >> d:\data\%deviceName%-SWUpdate.log

d:\53NTCSP\setupc /f /t:%devicename% /r BP000061.XML >> d:\data\%deviceName%-SWUpdate.log

if "%errorlevel%" == "2" set exists_error=yes

GOTO ENDFLASH

:ENDFLASH

if "%exists_error%" == "yes" echo Attention! There has been an error in the procedure on %devicename% >> d:\data\%deviceName%-SWUpdate.log

echo Installation complete >> d:\data\%deviceName%-SWUpdate.log

echo See the C:\CPQSYSTEM\LOG\CPQSETUP.LOG installation log file on each target server for details >> d:\data\%deviceName%-SWUpdate.log

echo End ===== >> d:\data\%deviceName%-SWUpdate.log

EXIT
```

Choosing the appropriate batch file

It is important to note that both of these batch files will get the job done. It is just a question of which approach you prefer. If you do not want to go to the trouble of creating batch files for each ProLiant Support Pack that you plan to distribute, use the swupdate.bat approach. If you plan to have people other than yourself deploying the Support Pack, and they may not know the proper variable values, use the alternative approach. Of course, users may also choose to create a hybrid approach that incorporates elements of both of these batch files.

There are also some important security implications to each of these approaches. In either case, the Insight Manager 7 service is configured to run under the context of an Administrator level account, and you may need to reconfigure the Insight Manager 7 service when the existing account password expires.

Using swupdate.bat allows you to configure the administrator username/password at the time you configure the task. This password will also need to be changed when the existing account password expires. Note that in no case is the password that is used to authenticate to remote servers stored in clear text; however, the password is stored in the Insight Manager 7 database, and will be presented in clear text to anybody editing the application launch task.

The information in this document is subject to change without notice.

MS, Windows and Windows NT are trademarks of Microsoft Corporation in the U.S. and/or other countries.

Other product names mentioned herein are trademarks of their respective companies.

© 2001, 2002 Hewlett-Packard Development Company, L.P.

11/2002

5981-4753ENA1
